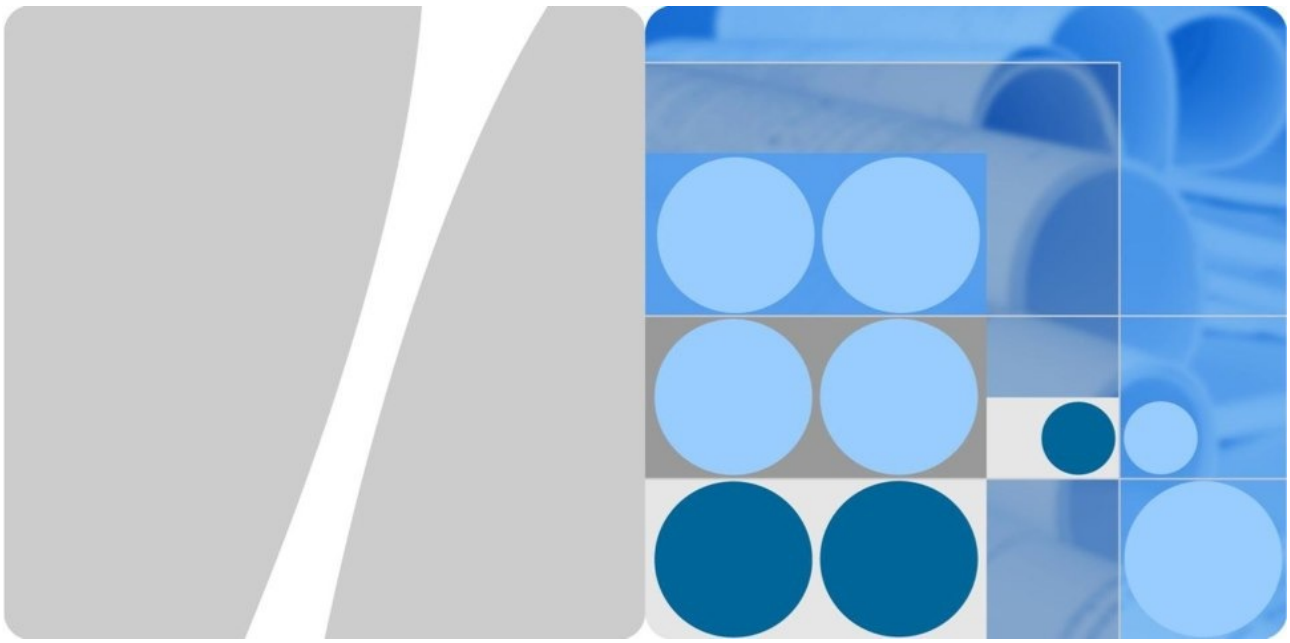


HUAWEI S12700 Agile Switch

Техническое описание

Документ предназначен для технических специалистов, а также продавцов для ознакомления с техническими особенностями и деталями инновационной разработки компании Huawei, которая открывает новую линейку продуктов Agile-коммутаторов.

В документе описана функциональность и техническая информация о коммутаторе Huawei S12700 в текущей модификации V200R005C00, а также планируемых модификациях, предполагающих расширение списка интерфейсных модулей. Документ может использоваться в качестве шаблона для формирования коммерческих предложений, а также, как техническое описание продукта для передачи заказчику.

http://enterprise.huawei.com/ru/
HUAWEI TECHNOLOGIES CO., LTD.

Содержание

Современные требования ИТ

Новые сервисы BYOD (Bring Your Own Device), Интернет вещей, видео, Big Data вносят свои требования к корпоративным сетям, а следовательно и к технологиям Ethernet коммутации :

Полная программируемость, SDN

Постоянное развитие протоколов и способов обработки данных вносит требование гибкости конфигурации сетевого оборудования. Применение программируемых микропроцессоров на базе технологии ASIC (Application Specific Integrated Circuit – интегральных схем специального назначения) решает задачу высокоскоростной передачи данных на аппаратном уровне (hardware forwarding). Однако функциональность ASIC ограничена выполнением специфического круга задач, например, поддержка фиксированного стека протоколов. Внедрение новых алгоритмов потребует замены аппаратного решения, либо будет реализовано в отдельном сервисном модуле, удорожающем стоимость решения и увеличивающем время внедрения. В отличии от этого, технологии Huawei позволят защитить инвестиции и внедрять новые услуги программным путем, без необходимости замены аппаратной платформы.

С точки зрения тренда программно-конфигурируемых сетей SDN (Software Defined Networking), корпоративным сетям потребуются высокопроизводительные устройства, способные реализовывать множество сетевых политик обслуживания для различных потоков трафика, относящихся к уникальным пользователям, приложениям и сетевой безопасности. Ключевые игроки рынка объявили о своей заинтересованности в стандартизации протокола OpenFlow, однако эта технология еще развивается и OpenFlow 1.3 претерпит ряд модификаций до начала повсеместного коммерческого внедрения кроссплатформенного подхода, обеспечивающего взаимодействие продуктов разных производителей. Эффективность SDN будет заключаться в возможности централизованного внедрения политик обслуживания и унификации архитектуры сети, поэтому сетевые элементы должны обладать максимальной гибкостью при высокой производительности обработки данных.

Интегрированное решение

Проникновение гаджетов в России приводит к необходимости принимать во внимание тренд BYOD, который предписывает ИТ службе не препятствовать подключению к корпоративной сети личных мобильных телефонов, планшетов и компьютеров, а использовать их встроенные функции (почту, календарь, веб) для внутреннего взаимодействия. Мобильности пользователей способствует развитие технологий беспроводного доступа LTE и WiFi в стандарте IEEE 802.1ac. Традиционные подходы к построению корпоративных сетей предполагают сегментацию сетевых ресурсов и внедрение сложных схем контроля доступа и сетевой безопасности. Рост затрат на развитие и эксплуатацию сети может оказаться экономическим стопором в развитии внутренних ИТ сервисов. В противовес этому, интеграция, упрощение топологии, конвергенция между проводными и беспроводными сетями, управление пользователями, их правами доступа и реализация унифицированных политик безопасности в решении Huawei S12700 Agile Switch, позволят существенно снизить стоимость владения сетью.

IP ресурсы

По прогнозу в 2015 году к сети Интернет будет подключено около 3.3 миллиарда терминалов, из которых 70% будут связаны с услугами «Интернет вещей». Развитие коммуникаций от машине к машине M2M (Machine-to-machine) и IPv6 принесет услуги для промышленности, энергетики и транспорта. В решении Huawei заложена возможность поддержки большого объема адресных записей IP и обеспечения политик обслуживания для существенного количества пользователей, чтобы обеспечить защиту инвестиций заказчика в перспективе 5–10 лет.

QoS

Современные протоколы передачи информации широкополосного видео требовательны к производительности сети, задержкам и потерям данных. Однако они не обеспечивают механизмов контроля и восстановления информации при сетевых проблемах. Для предотвращения перерывов в обслуживании из-за существенных потерь пакетов (приводящих к пропаданию видео изображения или заполнения экрана синими квадратами), сетевые решения должны поддерживать всплески трафика и управление приоритетами и очередями. Это становится особенно актуально в разнородной сети федерального масштаба, состоящей из каналов различной емкости.

Реализация QoS на сетевом уровне является сложной технологической задачей, однако это необходимо для внедрения новых сервисов и определения возможности передачи данных через каналы IP сети. Один из способов решения – применение протоколов на базе стандарта ITU-T Y.1731, который обеспечивает передачу Ethernet OAM фреймов для определения статистики односторонних или двунаправленных потерь данных и задержки для определения параметров производительности сети и локализации неисправностей. В сетях MPLS применяются стандарт ITU-T G.8113.1 для OEM коммуникаций, IETF RFC6374 и RFC6375, описывающие измерения задержки и потерь пакетов в MPLS сетях.

Современные методы управления ИТ в корпорациях предписывают необходимость гарантировать качество работы приложений для внутренних заказчиков. Поэтому во время предоставления услуги, сеть долж-

на обеспечивать принятие решений о распределении нагрузки и использовании резервных каналов для сохранения гарантированного уровня качества, что позволяет реализовать технология Huawei iPCA (Packet Conservation Algorithm for Internet – алгоритм сохранения пакетов в Интернет). Это новая разработка, которая идет далее традиционных механизмов Huawei для анализа качества сети (NQA, Network Quality Analysis) или агентов для гарантий обслуживания Cisco (SAA, Service Assurance Agent), выполняющих непрямые измерения качества.

Кампусная сеть следующего поколения от Huawei

В августе 2013 Huawei Enterprise аннонсировал новую линейку продуктов для кампусов следующего поколения, включающую:

- Контролер сети – Smart Campus Controller, который реализует координацию и управление сетью кампуса на основе политик обслуживания. Он обеспечивает унифицированную аутентификацию пользователей и контроль пути передачи трафика, выстраивая топологию сети и ресурсов.
- Коммутаторы S12700 Agile Switches, которые маршрутизируют трафик и реализуют политики обслуживания, как предписывает контроллер. Для достижения большой плотности высокоскоростных интерфейсов с возможностями сложной обработки трафика Huawei разработал новые сетевые процессоры Ethernet – (ENP, Ethernet Networking Processor). Коммутаторы доступны в двух сериях S12712 и S12708 на 12 и 8 линейных карт соответственно.
- В планы Huawei на начало 2014 входит использование ENP процессоров для коммутаторов линейки S9700 и S7700, а также других устройствах для организации доступа. Таким образом предполагается расширить функциональность Agile-коммутаторов на все продукты для построения LAN в кампусе.

Новая линейка коммутаторов отражает работу Huawei по развитию SDN, обеспечивая преемственность с традиционными сетями, полную программируемость и возможность быстрого внедрения новых сетевых технологий.

В отличии от традиционных сетей, где политики обслуживания определяются на основе сетевых параметров и конфигурируются на каждом сетевом устройстве, Huawei реализует подход к построению сети в котором сеть координируется и управляется из конца в конец, не разделяя доступ по технологиям – беспроводным или фиксированного доступа. При этом исключается необходимость администрировать каждое устройство или сервис.

Унификация фиксированного и беспроводного доступа

Кампусное решение Huawei комбинирует беспроводный и проводной доступ и унифицирует подход к топологии сети, аутентикации пользователей, реализации политик обслуживания и QoS. Это обеспечивается за счет встроенных BRAS и контроллера беспроводного доступа, реализованных непосредственно на линейных платах ENP – распределенное иерархическое решение виртуальной супер-фабрики (SVF – super virtual fabric), обеспечивающее единообразие в обработке и передачи данных различных сред доступа.

Традицонно беспроводные сети строились как дополнение к проводному LAN, поскольку не предоставляли достаточной пропускной способности и качества, а администрирование большого числа пользователей требовало существенных инвестиций в дополнительное оборудование, необходимость которого Huawei исключил.

С SVF администраторы сети могут обслуживать беспроводные и проводные сети как единый большой коммутатор, назначая универсальные политики на уровне пользователя.

Политики QoS на уровне пользователя

Динамический контроль потоков, планирование маршрутов передачи данных и назначение QoS обеспечивается Контроллером Кампуса, а реализуется Agile-коммутаторами. Политики могут назначаться для группы пользователей и приложений, чтобы сеть автоматически устанавливала соответствующие требования к передаче данных. Например, видео трафик получит больший приоритет, чем электронная почта, а группа разработчиков – больший, чем гостевые пользователи. Политики могут варьироваться в зависимости от расположения пользователя, времени суток и типа устройства доступа.

Мониторинг и управление

В традиционной сети администратор оперирует с топологией, содержащей физические порты и устройства. В решении Huawei администратор работает с пользователями, которые в процессе аутентификации могут определяться на различных портах и вовлекать как фиксированый, так и беспроводный доступ. Политики и права привязываются к пользователю и назначаются на порт за которым он распознан. Это существенно снижает операционные задачи по администрированию, обеспечению качества и безопасности.

Для централизованного управления качеством приоритетных приложений, Huawei разработал инновационый алгоритм сохранения пакетов в Интернет iPCA (Packet Conservation Algorithm for Internet). iPCA автоматически определяет потоки критичного трафика, предотвращая влияние потерь и участков сети с низкой скоростью. В отличии от традиционных технологий, iPCA позволяет диагностировать и локализовать аварии в сети, а затем перенаправить трафик пользователя так, чтобы продолжить непрерывность обслуживания.

Безопасность

Функциональность Agile-коммутаторов S12700 включает поддержку встроенных файрволов, NAT, IPSec, IPS, SSL VPN и защиту от DDoS атак.

В решении по предотвращению DDoS (distributed denial of service) атак применяется метод идентификации и изоляции вовлеченных сетевых ресурсов, в которых располагаются источники атаки. Попытка атаки блокируется на уровне доступа, сохраняя работоспособность остальной части сети.

Аутентикация с учетом месторасположения (LAA – location-aided authentication) может применяться для определения политик доступа. Например, при нахождении вне кампуса пользователю может быть отказано в доступе.

Инновации Huawei

T-bit AC

В рамках развития корпоративных WiFi решений, а также под воздействием BYOD, беспроводные сети из наложенного решения для посетителей кампуса превращается в основную сеть для производственных задач. Высокоскоростные стандарты (например 1.3 GBit/s IEEE 802.11ac) позволяют использовать WiFi не только для приложений с best-effort качеством, но и для широкополосного видео Telepresence, бизнес-критических приложений, видео-наблюдения. Увеличение скорости WiFi пользволит обеспечить единый уровень обслуживания вне зависимости от способа подключения к сети – через гигабитный Ethernet или беспроводную сеть.

Превращение WiFi в производственную среду приводит к необходимости создания полного покрытия в масштабах кампуса, а также обеспечения удаленного доступа. Это увеличивает количество точек доступа (AP – access point) до сотен и тысяч, приводит к необходимости внедрять решения по контролю за абонентами, а недостаток масштабируемости традиционных контроллеров доступа (AC – access controller) приводит к увеличению административных расходов и отсутствию возможности экономии на масштабе внедрения. Кроме того, при внедрении технологий гигабитного доступа, производительность и пропускная способность контроллера становится узким местом сети и причиной неудовлетворенности пользователей. Причины:

- Недостаток производительности для IEEE 802.11ac – покрытие среднего кампуса и филиалов требует порядка 1000 AP, принимая коэффициент переиспользования 1:3 производительность AC должна составлять 433 Gbit/s. Однако, традиционные AC обеспечивают 10 Gbit/s, поскольку изначально предназначены для сетей IEEE 802.11b/g/n.
- Масштабируемость контроллеров доступа приводит к необходимости сегментировать сеть кампуса, разделяя её между отдельными AC, планировать потоки трафика, что приводит к уменьшению эффективности, снижению возможности переиспользования ресурсов. Поскольку AC поропускает через себя трафик сети доступа, то резервирование устройств возможно только по кластерным схемам 1+1. Резервирование N+1 приводит к необходимости сложной синхронизации управляющей информации и перенаправления данных, перерывам в предоставлении услуг при авариях и регламентных работах.
- Внедрение беспроводных сетей, как наложенных на проводные, приводит к необходимости независимого администрирования пользователей и политик обслуживания (особенно касательно объема данных в условиях недостаточности пропускной способности). Подключение внешних устройств AC[1] требует адиминистрирования дополнительных портов, организации маршрутизации и других задач управления топологией сети.

T-bit AC и BRAS встроенные в ENP

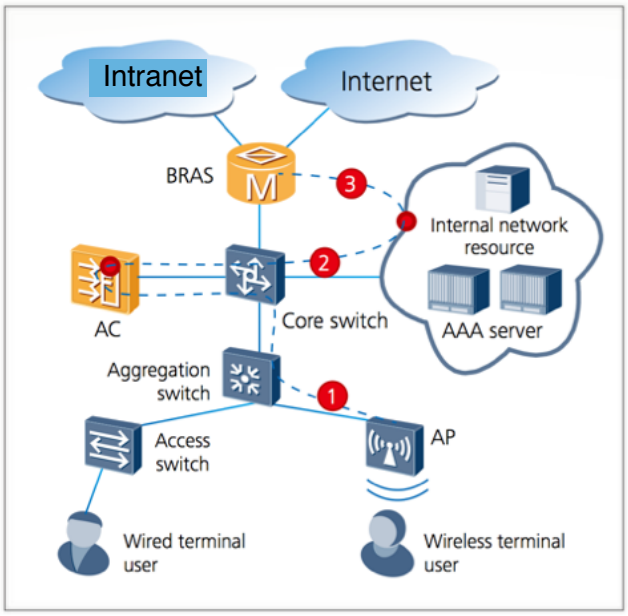
В Agile коммутаторах Huawei S12700 перечисленные проблемы решаются на основе функциональности AC интегрированной в высокопроизводительный Ethernet

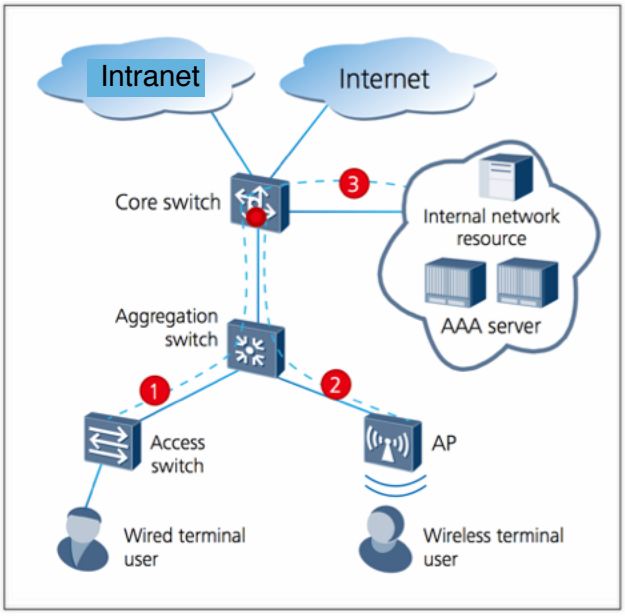
[1] даже AC встроенные в коммутаторы, исполняются как ACU (access controller unit) и являются независимыми сетевыми устройствами, а интеграция в коммутатор осуществляется за счет использования общего электропитания и (опционально) общей шины данных, при том что в некоторых исполнениях может требовать подключения физических портов

Network Processor (ENP) – непосредственно на интерфейсных платах, используемых для подключения агрегирующих коммутаторов или непосредственного подключения IEEE 802.11ac AP. Особенности и преимущества решения:

- Каждая плата серии X1E, использующая ENP процессор – Ethernet Service Interface Cards (SIC), объединяет коммутацию и функциональность AC, обеспечивая при этом скорость форвардинга 80 Gbit/s. В режиме полной загрузки устройство может пропускать до 800 Gbit/s[2] данных беспроводного доступа и обслуживать 4000 AP.
- Управление инкапсуляцией Layer 2 и Layer 3 происходит в решении Huawei посредством стандартного протокола CAPWAP (Control And Provisioning of Wireless Access Points – управление и настройка беспроводных точек доступа, RFC 5415), который позволяет автоматически настраивать работу AP в режиме прозрачной передачи данных к AC.
- Встроенный AC полностью интегрирован, не требует IP администрирования и не занимает отдельного слота в шасси коммутатора, не увеличивает потребляемую мощность устройства. Его распределенная архитектура позволяет обработать весь трафик сети доступа и обработать его непосредственно в интерфейсном модуле. Увеличение числа AP в сети не приводит к необходимости планирования ресурсов AC и сегментации сети – заказчик просто добавляет новую интерфейсную плату или подключает AP к свободному порту.
- Проведя аутентификацию пользователя и инкапсуляцию данных на ENP, трафик абонентов беспроводного доступа не будет ничем отличаться от трафика фиксированного LAN доступа. Таким образом обеспечивается реальная конвергенция между технологиями доступа, унифицируется архитектура, централизовано применяются универсальные политики обслуживания пользователей.
- Использование CAPWAP позволет внедрять AP и коммутаторы доступа без необходимости тонкой настройки конфигугации (zero-configuration deployment). Коммутатор Huawei S12700 управляет версиями файлов конфигурации AP и коммутаторов доступа. Проведение регламентных работ по замене конфигурации, программного обеспечения или установки патчей происходит автоматически путем анализа активности пользователей и числа активных точек доступа. Это приводит к минимизации потерь в обслуживании при масштабном внедрении изменений.
- Оперативная замена вышедшего из строя оборудования происходит без необходимости настройки – программное обеспечение и конфигурация нового устройства автоматически назначается аналогичной выбывшему.

Распределенный иерархический AC – решение Huawei для растущей емкости WLAN[3], унификации сетей, снижения капитальных и операционных затрат ИТ. Выделенные элементы AC и BRAS исключаются. Рост сети обеспечит экономию на масштабах и не приведет к усложнению эксплуатации. А использование стандартов, поддерживаемых ведущими производителями, позволит внедрять решение Huawei в качестве магистрального коммутатора, поддерживая преемственность и сохраняя ранее сделанные инвестиции.





[2] в материалах Huawei указывается цифра 960 Gbit/s, которая основывается на том, что все 12 слотов коммутатора будут заняты для подключения сети доступа

[3] 1.3 Gbit/s для IEEE 802.11ac основаны на использовании 3x3 MIMO, однако при переходе на 4x4 MIMO на частоте 160 МГц, возможно достигнуть скорости 3.5 Gbit/s

Эволюция к SDN

Huawei – активный участник Open Networking Foundation – ограницации занятой стандартизацией технологии SDN и протокола OpenFlow. По мнению Miercom, Huawei продемонстрировал один из первых примеров практического применения SDN, а реализация технологии POF (Protocol Oblivious Forwarding – форвар-динг вне зависимости от протокола), существенно более продвинута, по сравнению с оригинальным OpenFlow 1.3, хотя и обратно совместима со стандартом.

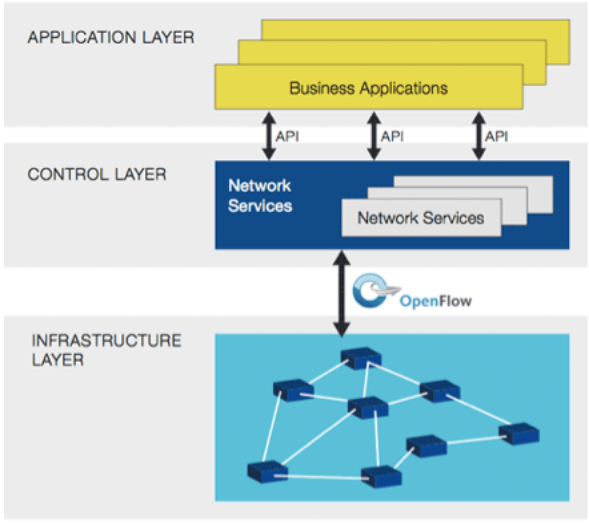
OpenFlow 1.3

В архитектуре SDN[4], уровень управления и передачи данных разъединены, сетевой интеллект и мониторинг логически централизованны, а управляемая сетевая инфраструктура не связана с приложениями. Решения SDN, основан-ные на протоколе OpenFlow в настоящее время внедряются в различном сете-вом оборудовании и программном обеспечении, предоставляя существенные преимущества, такие как :

- централизованное управление и контроль сетевых устройств различных производителей;
- единый API для описания требований к сетевой конфигурации со стороны приложений;
- быстрые инновации посредством внедрения новых сетевых возможностей и услуг без необходимости конфигурировать индивидуальные устройства или ожидать новые модфикации устройств от производителей;
- программируемость не только средствами производителей оборудования, но и операторов, корпоративного ИТ, независимых производителей программного обеспечения и пользователей за счет общей программной среды;
- улучшения в безопасности и надеж-ности сети, как результат центра-лизованного и автоматического управления сетевыми устройства-ми, унифицированной реализацией политик обслуживания и мини-мизации ошибок в конфигурации;
- возможность назначения политик для сессии данных, пользователя, устройства или приложения;
- улучшения в обслуживании поль-зователей за счет централизации информации о сети.

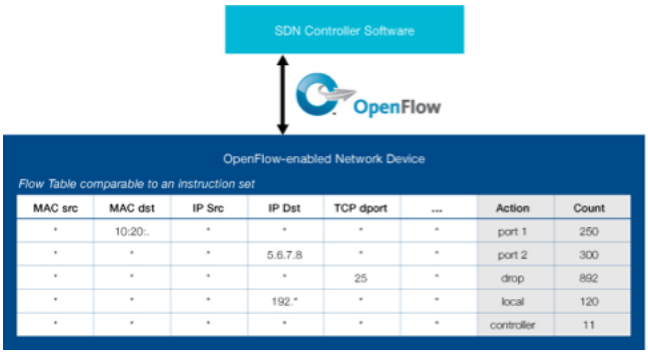
OpenFlow – интерфейс между уровнем управления и инфраструктурой, который обеспечивает прямой доступ и манипуляцию маршрутными таблицами сетевых устройств – коммутаторов и маршрутизаторов, физических или виртуальных (основанных на гипервизоре). OpenFlow работает аналогично программным инструкциям для настройки правил работы с потоками данных в коммутаторах. Определение потока включает MAC и IP адреса, номер VLAN, TCP и UDP порты и другую информацию. Назначение потоков аналогично определению списков контроля доступа и предписывает действия над потоком на каждом сетевом элементе. Действия включают направление форвардинга (указание порта), сброс, локальную коммутацию или маршрутизацию и другие. Список действий над трафиком выполняется поочередно, согласно установленных приоритетов.

Такой подход меняет требования к архитектуре и



функциональности:

- сетевые устройства становятся проще с точки зрения логики форвардинга – с них снимаются требования по реализаци протоколов маршрутизации, однако при этом сетевые устройства всегда должны поддерживать связь с контроллером, который определяет логику форвардинга – изменения должны затронуть всю логику управления сетью и конфигурацией;
- сетевые устройства вместо общей таблицы форвардинга на уровнях Layer 2 и Layer 3 должны использовать таблицу работы с потоками, которая может содержать набор параметров аналогичный пакетным фильтрам – дополнительная производительность по форвардингу, которая требует существенных аппаратных улучшений.



[4] Материалы об SDN подготовлены на основе открытой информации Open Networking Foundation https://www.opennetworking.org

Protocol Oblivious Forwarding

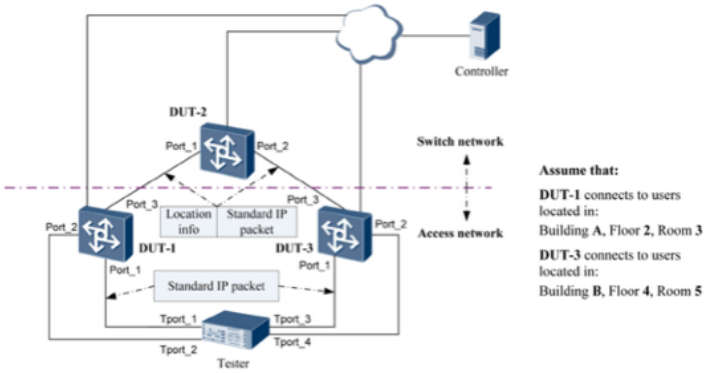
В своем решении Huawei предлагает заказчикам эволюционный путь внедрения SDN – в Agile-коммутаторах параллельно может существовать два уровня управления:

- традиционная коммутация и маршрутизация – работа схем резервирования, обеспечение локального взаимодействия равноправных устройств в надежном участке LAN, выполнение динамической маршрутизации для распределенной сети, фрагменты которой находятся за пределами зоны влияния централизованного ИТ (например интранет между различными компаниями), а также Интернет-маршрутизация и построение MPLS VPN,
- SDN – внедрение политик на уровне пользователей и/или приложений, управление безопасностью и качеством обслуживания, оптимизация пути трафика отдельных сетевых услуг.

Внедрение SDN в реализации Huawei может проходить плавно и поэтапно, не затрагивая работу существующих бизнес-решений и оставляя среди инструментов ИТ проверенные традиционные средства. Кроме того, если протокол OpenFlow описывает действия только над Ethernet и IP, то разработанный Huawei протокол POF позволяет определять параметры расширенного количества сетевых протоколов, в том числе открывая возможность по внедрению новых протоколов.

Существенной инновацией Huawei является аппаратная поддержка сложных сценариев форвардинга на ENP процессорах. Это позволяет реализовать управление потоками в SDN без ущерба производительности – коммутатор поддерживает до 16 миллионов потоков данных. Управление обеспечивается со стороны SDN контроллера – Smart Campus Controller, который в свою очередь предоставляет API для интеграции с другими системами и уровнем управления приложениями.

Внедрение новых протоколов, тесты новых RFC, добавление специфических параметров безопасности – задачи которые поддерживаются в POF и успешно протестированы Miercom, наряду с нагрузочными тестами. В частности была проверена возможность передачи нестандартных пакетов. Так к заголовку пакета на первом коммутаторе были добавлены параметры месторасположения пользователя. Второй коммутатор принимал решение о форвардинге на



основе таблицы потоков определенных пользователем, а затем удалял служебную информацию.

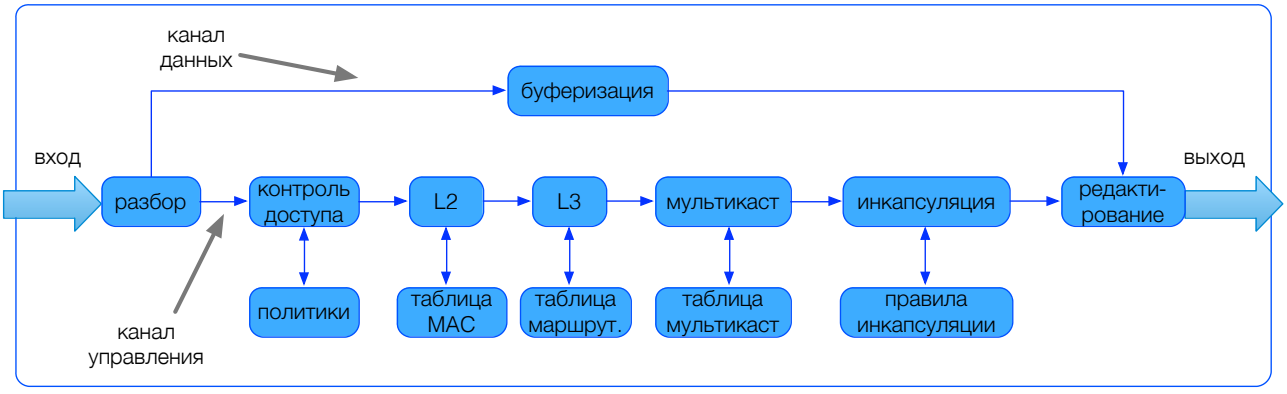
Выделение потоков данных от пользователей, физических или виртуальных серверов, или приложений позво-ляет отнести SDN в разряд технологий для построения VPN. В этом контексте говорят о возможности Huawei по построению SDN VPN в масштабах кампуса.

Новая аппаратная архитектура ENP

В качестве показателей для измерения производительности сетевого устройства могут выступать: пропускная способность, задержки, управляемость и безопасность. Среди прочих факторов, определяющим является технология передачи (различают программную и различные виды аппаратной реализации передачи данных).

С момента появления первого Ethernet коммутатора в 1989 году, производительность устройств увеличилась с 10/100 Mbit/s до 1 Gbit/s или даже 10 Gbit/s. В основе роста была технология ASIC. Однако, быстрый рост видео, мобильных рабочих мест, BYOD, облачных приложений и VDI (Virtual Desktop Infrastructure, инфраструктура виртуальных рабочих мест) и «Интернет вещей», вносит новые требования к Ethernet для обеспечения большей скорости, производительности, знания специфики пользовательскго поведения и контента, простого управления и реализации политик обслуживания.

Современные коммутаторы поддерживают функции Layer 3 IP маршрутизации, однако преимущественно используются для агрегирования трафика абонент-



ских терминалов, поскольку не могут обеспечить внедрения новых сервисов необходимых для облачных технологий. Причина заключается в том, что микропроцессоры, построенные на ASIC технолгии поддерживают только предопределенные протоколы и фиксированный механизм передачи данных. Модификация алгоритмов обработки происходит программным путем лишь в рамках стандартной модели, как показано на рисунке ниже.

Микропроцессры ASIC обрабатывают данные только предопределенных протоколов. Именно поэтому внедрение нестандартных Ethernet фреймов (в частности с инкапсуляцией), вызывало у производителей сложности с поддержкой высокой производительности и необходимость выпуска новых модификаций аппаратных решений. Так, добавление новых сервисов, приводило к редизайну микросхем и последующим изменениям в производстве, включая: моделирование, создание прототипа, тестирование – процессы которые могли длиться до нескольких лет. Таким образом, производители были ограничены в скорости внедрения новых сервисов.

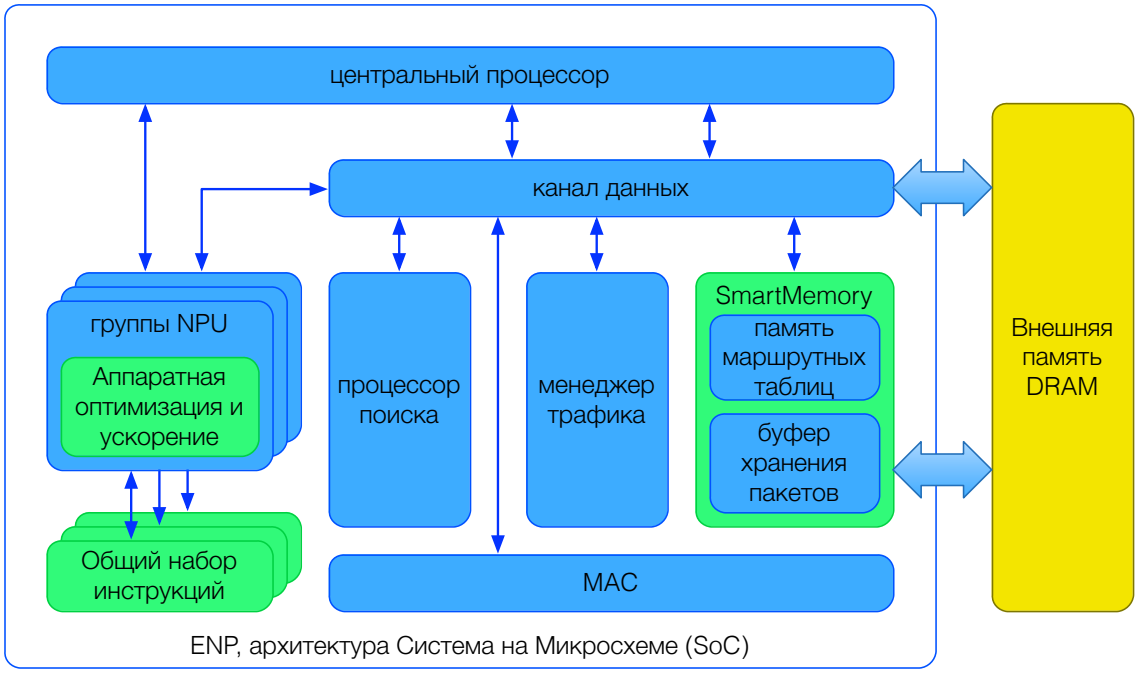
Коммерческие сетевые процессоры NP (Network Processors) пришли, на смену ASIC микропроцессорам. Смогут ли они стать решением для Ethernet коммутаторов?

Коммерческий NP состоит из модулей сетевой обработки (NPU, Network Processing Unit), памяти для инструкций/алгоритмов обработки (instruction memory), памяти для маршрутных таблиц (table memory), памяти для хранения пакетной нагрузки – данных инкапсулированных пакетов верхних уровней (packet memory), и таблиц внешней памяти DRAM (Dynamic Random-Access Memory, динамической памяти произвольного доступа). Такой дизайн обладает большей гибкостью по сравнению с ASIC, является программируемым на уровне инструкций обработки данных, однако размер инструкций в каждой группе NPU ограничен и новые сервисы должны вписываться в эти ограничения. Производительность одного или нескольких NPU занятых высоконагруженными задачами, также может стать ограничением.

Высокая производительность и гибкость

Микропроцессоры ASIC обладают высокой производительностью (+), низким энергопотреблением (+), но негибкой архитектурой (-), коммерческие NP обладают гибкостью (+), но низкой производительностью (-) и высоким энергопотреблением (-). Результатом более чем 20-и летнего опыта Huawei в разработке микропроцессоров стал инновационный сетевой процессор Ethernet (ENP, Ethernet Network Processor), который объединяет в себе высокую производительность микропроцессоров ASIC и гибкость коммерческих NP.

Дополненная область инструкций по обработке трафика в сочетании с аппаратным ускорением и низким энергопотреблением компенсируют недостатки коммерческих NP. При этом ENP использует общую память для инструкций по обработке трафика и каждая из групп NPU может выполнять любую из задач, включая Parse, Search I, Resolve, Search II и Modify. В ENP е требуется разделять отдельные сервисы по отдельным группам NPU, а технология параллельной обработки позволяет выполнять сложные задачи обработки трафика без потери производительности.



ENP, архитектура Система на Микросхеме (SoC)

SmartMemory – оптимизация быстродействия памяти

Коммерческие NP и микропроцессоры ASIC разделяют области памяти для хранения адресации и данных, при необходимости взаимодействия возникает дополнительная задержка в обработке данных. А одновременный доступ разных процессов к одной и той же

области памяти приводит к блокировке для сохранения консистентности данных.

Huawei ENP используют интегрированную память SmartMemory, который интегрирует память для хранения данных, адресации и расчетов. Такой подход снижает время обмена и приводит к росту быстродействия всей системы.

Решение SmartMemory интегрирует в себе систему поиска разработки Huawei, сопроцессор и менеджер трафика. Он обеспечивает все алгоритмы поиска, расчетов и чтения-записи так же как коммерческие процессоры или микропроцессоры ASIC, с той разницей, что в решении Huawei, все эти алгоритмы могут быть использованы любым функциональным модулем ENP.

Миллионы адресных записей и гибридный OpenFlow

Будучи активным разработчиком SDN решений, Huawei создал расширение стандарта OpenFlow – технологию Protocol Oblivious Forwarding (POF), обратно совместимую с OpenFlow, иначе называемую гибридным OpenFlow. Этот подход обеспечивает возможность использовать как OpenFlow, так и традиционные механизмы маршрутизации для передачи и управления трафиком. Таким образом, заказчик получает возможность осуществить плавную миграцию к SDN. Процессоры ENP реализуют программное наращивание функциональности и поддерживают до 16 миллионов потоков данных OpenFlow, наряду с выполнение традиционной коммутации и маршрутизации.

Снижение потребляемой мощности за счет ENP

Одним из способов снижения потребляемой мощности в ENP является комбинирование нескольких задач в одном микропроцессоре. Так традиционная архитектура коммутаторов предполагает наличие в интерфейсном модуле как минимум двух элементов памяти – один для управления передачей данных (форвардинга трафика), другой – для организации буфера передаваемых данных. Их взаимодействие увеличивает время обработки, поскольку каждый из элементов требует дополнительной мощности. В решении Huawei эти задачи совмещены в единой SmartMemory, комбинирующей обе области памяти, увеличивающей быстроту операций и снижающей энергопотребление.

Энергопотребление микросхемы обычно включает 40% статической и 60% динамической мощности. Статическое энергопотребление пропорционально рабочему напряжению транзисторов. Микропроцессор ENP использует продвинутый контроллер напряжения, который позволяет снизить статическое энергопотребление. Снижение рабочего напряжения транзисторов происходит в процессе производства микросхем.

Изменение рабочей мощности транзисторов и частоты процессора позволяет снизить динамическое энергопотребление. Настройкой частоты в реальном времени руководит интеллектуальный спидометр, который обеспечивает регулировку в зависимости от объема передаваемых данных за счет изменения скорости поступления данных к группам NPU – это прямопропорционально влияет на показатели энергопотребления. ENP может аппаратно полностью отключать некоторые группы NPU, для снижения энергопотребления.

Надежность

Существенными нововведениями в реализации качества в Agile-коммутаторах Huawei S12700 стали :

- Новая технология CSS2 для организации кластера – улучшения в производительности, минимизация управляющего оборудования;
- Технология iPCA для сквозного мониторинга бизнес-критических данных.

Кластеризация CSS2

Технология реализации кластера CSS2 наследует аппаратную реализацию объединения коммутационной матрицы для обесечения сетевой надежности. Современные высокопроизводительные коммутаторы обеспечивают высокую степень надежности центрального процессора, интерфейсных и сервисных модулей, электропитания и охлаждения. Кроме того, надежность сети зависит от правильной организации сетевой архитектуры. В отличии от такого подхода, Huawei реализовал для коммутаторов S9700/S7700 инновационную схему CSS (Cluster Switching System – система кластерной коммутации), направленную на обеспечение сетевой надежности посредством объединения систем через интерфейсы кластеризации. Решение CSS2 (Cluster Switch System Generation 2 – система кластерной коммутации второго поколения) в коммутаторах Huawei S12700 базируется на CSS и реализует кластерные соединения для каждого SFU посредством модуля кластеризации 8x10GE – общая емкость кластерных соединений 640 Gbit/s. В будущем планируется использовать кластерные модули 6x40GE и утроить емкость кластера до 1.92 Tbit/s. Технология CSS предполагает двукратную передачу данных, а CSS2 передает данные между шасси только один раз. Задержка, вносимая кластером CSS2

составляет 21 µs – лучший показатель в индустрии, в среднем на 40% меньше чем в среднем по аналогичным решениям.

Оптимизация капитальной стоимости решения достигается за счет схемы резервирования MPU в кластере 1+N, то есть для работоспособности кластера достаточно чтобы MPU был хотябы в одном шасси. Это нововведение по сравнению с CSS, где требовалось наличие MPU в каждом шасси.

iPCA – мониторинг высокоприоритетных данных

Сервисы видео, голоса, доступа к облачным ресурсам, VDI, чувствительны к качеству и требуют сквозного измерения (E2E, End-to-End) и гарантий. Однако, диагностика уровня качества сети представляет нетривиальную задачу для ИТ менеджмента, поскольку сеть не представляет инструментов оценки рисков и идентификации мест деградации качества обслуживания.

Индустриальные решения выполняют непрямые измерения путем вставки служебных пакетов в поток клиентского трафика с последующим расчетом параметров качества :

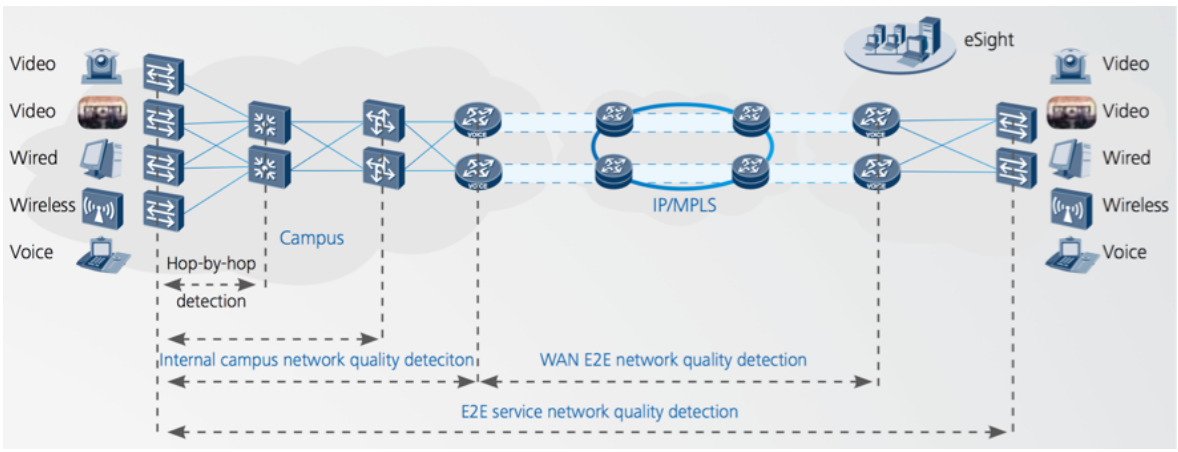
- ITU-T Y.1731 – OAM протокол уровня Ethernet, который выполняет сбор статистики потери трафика в прямом или прямом+обратном направлении – это позволяет определить уровень качества и локализовать аварии;
- ITU-T G.8113.1 – OAM протокол для MPLS-TP, кроме того для MPLS существуют IETF RFC6374 (Packet Loss and Delay Measurement for MPLS Networks) и RFC6375 (a Packet Loss and Delay Measurement Profile for MPLS-Based Transport Networks) для сбора MPLS статистики и локализации аварий;
- Для IP сетей существуют RFC5357 (a Two-Way Active Measurement Protocol) и RFC4656 (a One-way Active Measurement Protocol (OWAMP)) для статистики и локализации аварий;
- Частные решения Cisco Service Assurance Agent (SAA) и аналогичный протокол Network Quality Analysis (NQA) от Huawei.

Недостаток непрямых методов измерения заключается в природе IP сети – connectionless (не привязана к соединениям), в связи с чем трафик измерений может направляться по другому пути чем трафик пользовательских данных.

В отличии от вышеперечисленных методов, iPCA технология (Packet Conservation Algorithm for Internet – алгоритм сохранения пакетов в Интернет) может оперативно определять потоки видео и голосового трафика и моментально распознавать аварии в сетевых каналах, платах и даже микропроцессорах, существенно увеличивая эффективность O&M.

Технология iPCA аппаратно реализована на процессорах ENP и производит мониторинг маршрута передачи данных за счет прямых измерений. Это позволяет измерять потери, задержки, джиттер, объемы переданного трафика, а также обеспечивает точную идентификацию аварий на каждом узле маршрутизации трафика (hop-by-hop fault detection).

Управление iPCA происходит со стороны серверов контроля измерений (measurement control servers), а реализуется на Agile-коммутаторах. На сервере определяется какой трафик подлежит диагностике, затем ENP процессоры вовлечены в задачу идентификации критичного трафика, проведения измерений и сбора статистики, выполнения расчетов и передачи отчетов на сервер. Приоритезация трафика обеспечивается за счет маркировки зарезервированного бита (бит 0 в поле флага) IPv4 заголовка пакета и не влияет на тип трафика. За счет простой маркировки, аппаратным



методом обеспечивается быстрая реализация приоритетной передачи.

В примере для корпоративной сети iPCA определяет показаетли производительности на доступе, аггрегировании, в ядре сети и отдельно в сегменте WAN сети. Диагностике подлежит каждый транзитный маршрутизатор и iPCA определяет параметры качества, а также локализует аварии. При этом, iPCA не дает возможности диагностики MPLS WAN сети, однако будучи реализованный на входе и выходе корпоративной сети, iPCA может определять аварии и качество в магистрали.

Сценарии использования

Корпоративная сеть

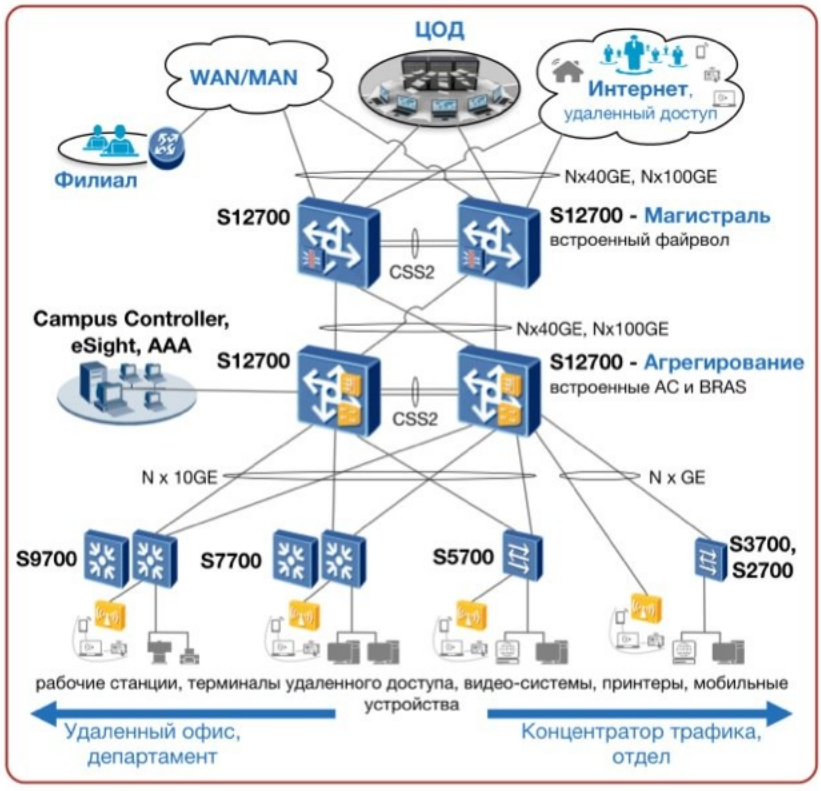
- *в 2012 году продано более 1 миллиарда смарт-терминалов*
- *в 2013 году число продаж WLAN чипов в мире достигло 1.7 миллиарда – 70% прирост по сравнению с 2012 годом*
- *аналитиками оценивается что 35% офисных работников использует беспроводные терминалы*
- *технолгия WiFi 802.11ac обеспечивает передачу данных со скоростью 1.3 Gbit/s, что приводит к требованиям терабитной пропускной способности магистрали*
- *срочная информация должна переда-ваться пользователям моментально – визиты заказчиков, расписание встреч, программы телеконференций, постановка проектных задач и другие.*

Развитие ИТ технологий принципиально меняет способы работы пользователей в корпоратив-ных сетях. Так, если 20 лет назад мы работали на стационарных компьютерах, 10 лет назад стали пользоваться портативными компьюте-рами, то сейчас мы всё больше работаем на смартфонах и планшетных устройствах – чаще собственных, чем предоставленных работода-телем. BYOD добавляет новые требования к пользовательским услугам, характеристикам и дизайну сети.

Коммутаторы Huawei S12700 для кампусных сетей обеспечивают :

- построение высокопроизводительного кампуса и ЦОД, агрегирующего до до 576xFE, 576xGE, 192x10GE, 96x40GE; в будущем расширяемый до 576x10GE или 96x100GE портов; 1.92 Tbit/s кластера.
- террабитный контроллер беспроводного доступа на 4 тысяч базовых станции;
- функциональность BRAS (Broadband Remote Access Server – сервер удаленного широкополосного доступа) для аутентикации пользователей и туннелирования абонентского трафика с целью обеспечения безопасности;
- автоматическое удаленное конфигурирование беспроводных AP и агрегирующих коммутаторов по технологии CAPWAP;
- безопасность внутренней сети интегрированными средствами: файрвол, IPSec, IPS, SSL;
- встроенную защиту от внешних угроз посредством NAT, файрвола и предотвращения DDoS; IPSec для криптографирования магистрального трафика и удаленного доступа;
- назначение политик ослуживания на уровне пользователя, управление потоками данных по технологии SDN,
- автоматическое распознавание, приоритезацию и локализацию аварий для приоритетного трафика, за счет технологии iPCA;
- виртуализацию пространства доступа к облачным приложениям, гарантии качества на основе иерархических пятиуровневых очередей;

Наличие встроенного контроллера беспроводного доступа и BRAS, возможности туннелирования и управления качеством в коммутаторе Huawei S12700 устраняют различие в топологии и принципам построения проводного и беспроводного сегмента сети, обеспечивая универсальные политики обслуживания пользователей вне зависимости от способа и места



подключения.

Многопользовательская образовательная сеть

Социальные сети зародились в университетах – facebook в Гарварде, вконтакте в СПбГУ). Коммуникации среди поколения-Y происходят чаще в социальных сетях и меседжерах, чем по телефону. Так, если в корпоративной среде важно внедрять средства унифицированных коммуникаций, то для образования важна поддержка Web 2.0 и социальных сетей – в том числе для задач обучения и взаимодействия преподавателей и студентов.

Современная практика образования предусматривает не только использование интернет (как коммуникацион-ной и информационой среды), а также, удаленное обучение, автоматизированную сдачу тестов и экзаменов. Сегодня доступ к информации структурирован в виде баз знаний и внутренних WiKi ресурсов, пополняемых пользователями в рамках Web 2.0 (интерактивных приложений для создания и модерации контента средствами пользователей). Дистанционное обучение сейчас включает не только видео, но и мультимедийное взаимодействие преподавателей и студентов, организацию виртуальных классов и предоставление информации высокой четкости (HD – high definition) всем участникам. Процесс обучения мигрирует в облачные сервисы, доступ к которым должен обеспечиваться постоянно, преимущественно с помощью беспроводных технологий.

Среднестатистический посетитель образовательного кампуса имеет до трех беспроводных устройств, процесс обучения и аттестации должен быть непрерывным, аутентикация пользователя однозначно определяет индувидума (в отличии от принятого в виртуальном социальном мире принципа непроверяемых никимен), в последующем, вся работа студента в сети должна быть контролируема и отслеживаема (traceable).

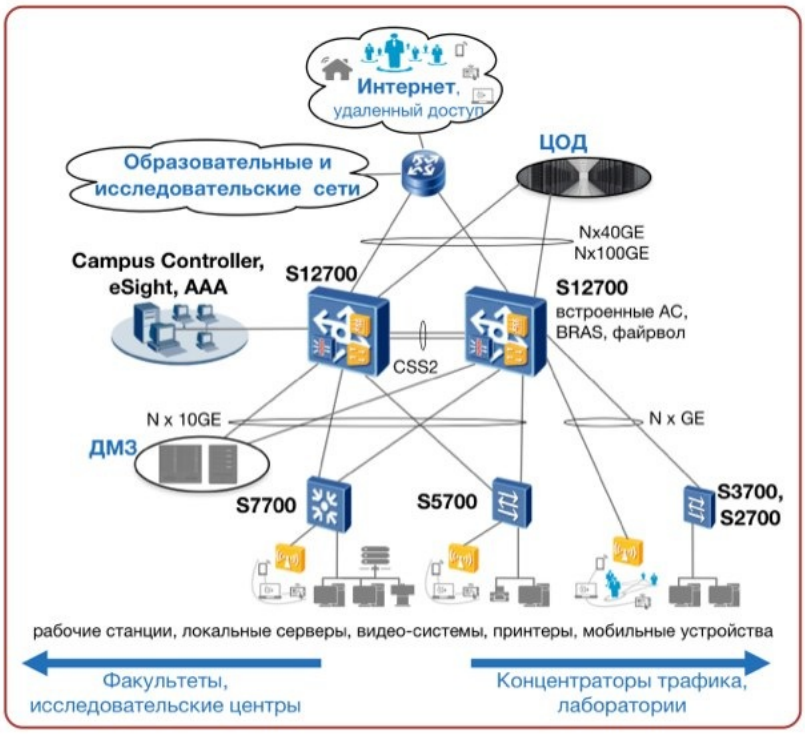
Решение Huawei Enterprise для образовательных кампусов актуально по причинам высокой производительности и возможностей для беспроводного доступа. Оно включает функции безопасности, аутентикации и качества, аналогично решению для корпораций. Отличие состоит в количестве мобильных пользователей – коммутаторы S12700 поддерживают до 65 тысяч одновременных подключений. При этом, если в корпорациях актуально решение задачи защиты данных от копирования (в том числе за счет VDI), то в образовательном кампусе предоставляется максимально полный доступ к информации. SSL криптография применяется для сокрытия лишь некоторых конфиденциальных данных.

Угрозы DDoS, вирусов и других вредноносных воздействий, могут происходить от пользователей. Поэтому, реализованные Huawei Enterprise решения по безопасности, применяются для защиты ядра сети и ЦОД как от внешних воздействий, так и внутренних.

Транспорт видео

Ведомственные решения и муниципальные сети видеонаблюдения отказываются от аналоговых технологий и развиваются в сторону IP систем и HD качества. Не обладая средствами контроля передачи данных, видео решения предъявляют высокие требования к качеству сети :

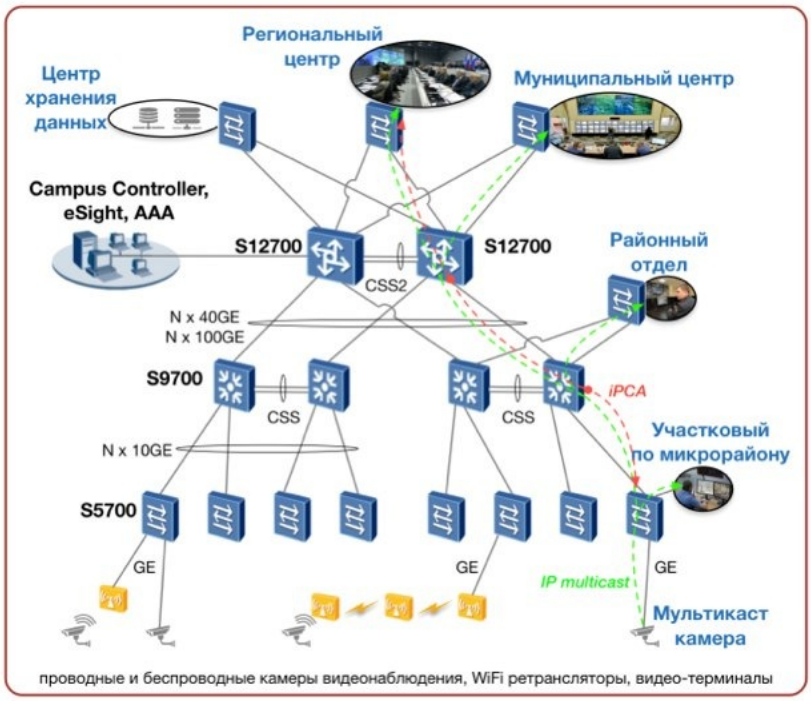
- Телеприсутствие – скорость 5 Mbit/s на каждый экран при качестве 1080P, джитер ≤ 10 мс, коэффициент потерь ≤ 0.05%,
- IP видеонаблюдение – скорость от 200 kbit/s до 3.5 Mbit/s на каждую камеру, джитер ≤ 10 мс, коэффициент потерь ≤ 0.05%, задержки ≤ 150 мс.



Сеть на основе коммутаторов Huawei S12700 предоставляет пропускную способность в 37.28 Tbit/s, которая может строиться по принципу дерева или с использованием кольцевой топологии, обеспечивающей восстановление сети в течение 50 мс за счет использования Smart Ethernet Protection (SEP) протокола. Фиксированные камеры могут подключаться непосредственно к портам коммутаторов, а беспроводные – агрегироваться сетью радио-доступа. Возможности работы с мультикасттрафиком позволяют подключать как обычные, так и широковеща-тельные камеры для передачи видео-потока одновременно в несколько ситуационных центров. Размер таблиц маршрутизации составляет 262 тысячи мультикаст записей, что покрывает потребности в количестве камер для крупной сети наблюдения.

Качество обеспечивается за счет :

- линейных плат коммутатора Huawei S12700, которые предоставляют буфер передачи данных объемом в 1.5 GB и



сохранение данных при всплесках трафика до 200 мс на каждом порту,

- кластерного решения CSS2 (Hardware Cluster Switching System 2) для высокоскоростного объединения коммутационной матрицы и центрального процессора,
- 1+N резервирования центрального процессора в рамках кластера,
- технологии iPCA, которая работает в масштабах сети коммутаторов Huawei S12700/S9700/S7700/S5700 и автоматически распознает потоки трафика, критичного к качеству, выстраивает этот трафик в приоритетные очереди,
- высокой скорости обработки данных при реализации сложных схем управления потоками данных на основе ENP процессоров,
- встроенных функций безопасности для защиты от вредоносных внешних воздействий и атак направленных на лишение работоспособности.

Корпоративная сеть городского масштаба

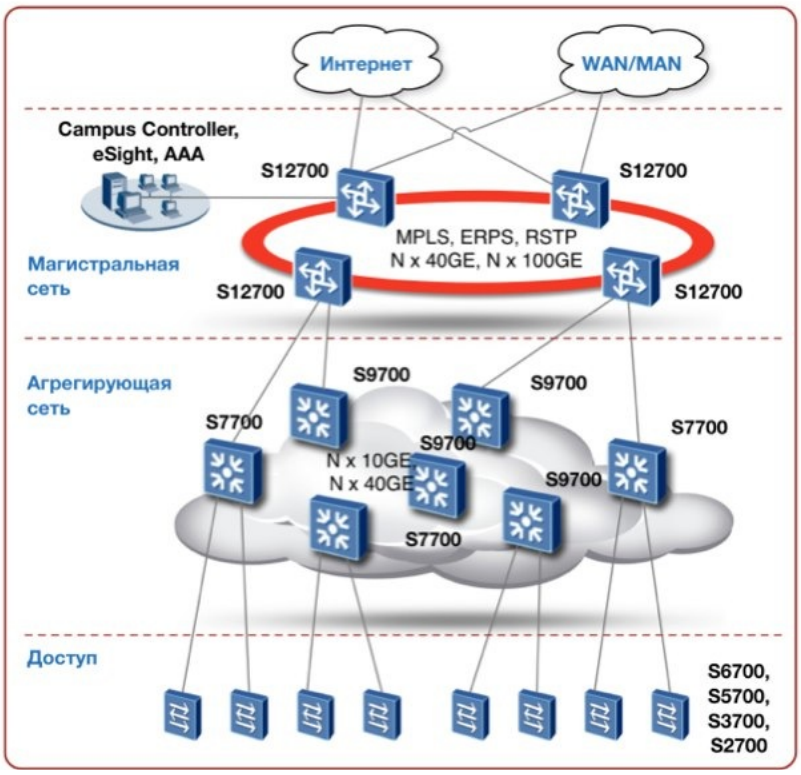
Коммутаторы Huawei S12700 обеспечивают высокую производительность и большую емкость таблиц маршрутизации (1 миллион MAC адресов, 3 миллиона маршрутных записей IPv4 и 1 миллион записей IPv6) для построения сети городского масштаба и Интернет маршрутизации. Магистральные каналы могут строиться по технологиям 100 GE с использованием как Ethernet коммутации и IP маршрутизации, так и MPLS для контроля потоков трафика и фрагментации сети с использованием технологии MPLS VPN.

Каналы доступа и подключения к другим сетям могут использовать интерфейсы 10 GE или 40 GE, соответствующая производитель-ность может достигаться на встроенных ресурсах обеспечения безопасности – NAT, файрвол, защита от DDoS атак.

Контроль качества для видео и других значимых приложений достигается за счет работы сквозного протокола определения потоков данных – iPCA, который назначает соответствующие приоритеты для реализации качества обслуживания.

Отличительной особенностью решения Huawei является управляемость решения и возможность миграции сети к SDN, которая будет возможна в масштабах всей сетевой линейки Agile-коммутаторов, включая S12700, а также S9700/S7700 и младшие модели оборудования. Возможность определения на кадом устройстве до 16 миллионов потоков данных, а также наличие 256 тысяч записей в списках контроля доступа (ACL – access control list), делают возможным организовать гибкий контроль над пользователями. Для этого Smart Network Controller позволяет определять политики обслуживания не только на уровне сетевых параметров, но и на уровне пользователей, которые проходят аутентификацию в сети и затем получают индивидуальный набор политик обслуживания и доступа к сетевым ресурсам.

Инвестируя в сеть на базе решения Huawei заказчик обеспечивает себя современным решением на ближайшие 5–10 лет за счет :



- высокопроизводительных интерфейсов доступа 10/40 GE, магистрали 100 GE,
- поддержки SDN и прозрачности функциональности в масштабах широкой линейки продуктов (согласно плана развития в 2014 году),
- активной работы Huawei по формированию стандартов и внедрению их в продуктах,
- собственная разработка микропроцессоров для обеспечения лидерства в производительности и функциональности, а также низкого энергопотребления.

Аппаратная архитектура

S12700 это полностью программируемый гибкий коммутатор, разработанный для кампусных сетей нового поколения. Системная архитектура S12700 разделяет управление услугами от коммутации данных и поддерживает резервирование коммутационной матрицы – модулей switch fabric units (SFU) в конфигурации N +1. В защищенном режиме один SFU может резервировать до трех работающих SFU. Использование в коммутаторе S12700 Huawei Ethernet Network Processor (ENP) обеспечивает :

- высокую производительность,
- большой объем адресных таблиц MAC, маршрутных записей IP и MPLS,
- большой размер буфера для передаваемых данных,
- встроенный T-bit AC – контролер WiFi базовых станций и BRAS.

Возможности программирования позволяют заказчику определять собственные сценарии коммутации и функциональность для тонкой настройки сети. Это позволяет унифицировать архитектуру сети для абонентов проводного и беспроводного доступа и обеспечить беспрепятственную эволюцию к SDN.

Аппаратная архитектура S12700 разделяет на уровень управления коммутацией, передачи данных и O&M. От младших моделей серии Sx700 – коммутаторов S9700 и S7700 новую разработку отличает изолированное исполнение MPU (Main Processing Unit – модуль центрального процессора) и SFU (Switching Fabric Init – модуль коммутационной матрицы). Резервирование центрального процессора выполняется по схеме 1+1 для шасси S12700 и по схеме N+1 для кластера из нескольких устройств, объединенных по технологии Huawei CSS2 (switch system generation 2 – коммутационой системы второго поколения). Это позволяет осуществлять замену нерезервированных MPU в кластере без влияния на передачу данных – за счет разделения уровней передачи данных от управления коммутацией и управления устройством, резервный MPU в другом шасси продолжит обеспечивать выполнение всех задач обработки протокольных данных маршрутизации и управления устройствами, передача данных сохранится, кластер не разделится. При этом, функции внутренней диагностики идентифицируют неисправность в работе системы за 10 милисекунд и восстанавливают работу всей системы за 50 милисекунд.

Четыре модуля коммутационной матрицы SFU обеспечивают пропускную способность 17,44 Tbit/s, которая может расширяться до 37,28 Tbit/s. Резервирование SFU выполняется по схеме 3+1 с балансировкой нагрузки между элементами коммутационной матрицы. Неисправность или регламентное извлечение одного из SFU не влияет на способность устройства передавать данные. При этом, дополнительная возможность по обеспечению резервирования заключается в кластеризации устройств с емкостью каналов между элементами кластера в 640 Gbit/s. В будущем эта величина увеличится в три раза – до 1920 Gbit/s.

Коммутатор S12700 выпускается в двух моделях:

- восьмислотовой S12708, обеспечивающий до 384xFE, 384xGE, 128x10GE, 64x40GE в текущей модификации коммутатора S12700 V200R005C00; при использовании линейных плат 48x10GE и 8x100GE, которые будут доступны в следующих модификациях программного обеспечения, восьмислотовое шасси обеспечит работу до 384x10GE или 64x100GE портов;
- двенадцатислотовой S12712, емкостью до 576xFE, 576xGE, 192x10GE, 96x40GE; в будущем расширяемый до 576x10GE или 96x100GE портов.

В зависимости от количества и скорости интерфейсов, линейные карты (LPU – Line Processing Unit) выполнены по трем сериям и соответствующим технологиям исполнения:

- Серия-S относится к SA и SC интерфейсным модулям, например 8-port 40G BASE-X optical interface card (SC, QSFP+); поддерживает 128 тыс. MAC адресов, до 38 тыс. ACL (Access Control List – пакетных фильтров IP), до 16 тыс. IP FIB (маршрутных записей IP);
- Серия-E включает EA и EC интерфейсные карты, например 48-port 100M/1000M BASE-X optical interface card (EC, SFP); поддерживает 128 тыс MAC адресов, до 1,5 тыс. ACL, до 128 тыс. IP FIB;
- K серии-X1E относятся ENP интерфейсные карты, например 8-port 10G BASE-X optical and 8-port 100M/1000M BASE-X optical and 8-port 10M/100M/1000M BASE-T combo electrical interface card (X1E, RJ45/SFP/SFP+); этот тип карт поддерживает 1 миллион MAC адресов, до 64 тыс. ACL, до 3 миллионов IP FIB.

Основным элементом интерфейсных карт серии-X1E является инновационная разра-ботка Huawei – ENP процессор, обеспечивающий высокую производительность, 1,5 GB буфер передачи данных, превращающий коммутатор в эффективный инструмент для построения сетей распространения видео-приложений, и данных критичных для бизнес-задач. Карты серии-X1E выполняют сложную обработку данных и предназначены для подключения агрегирующих ком-

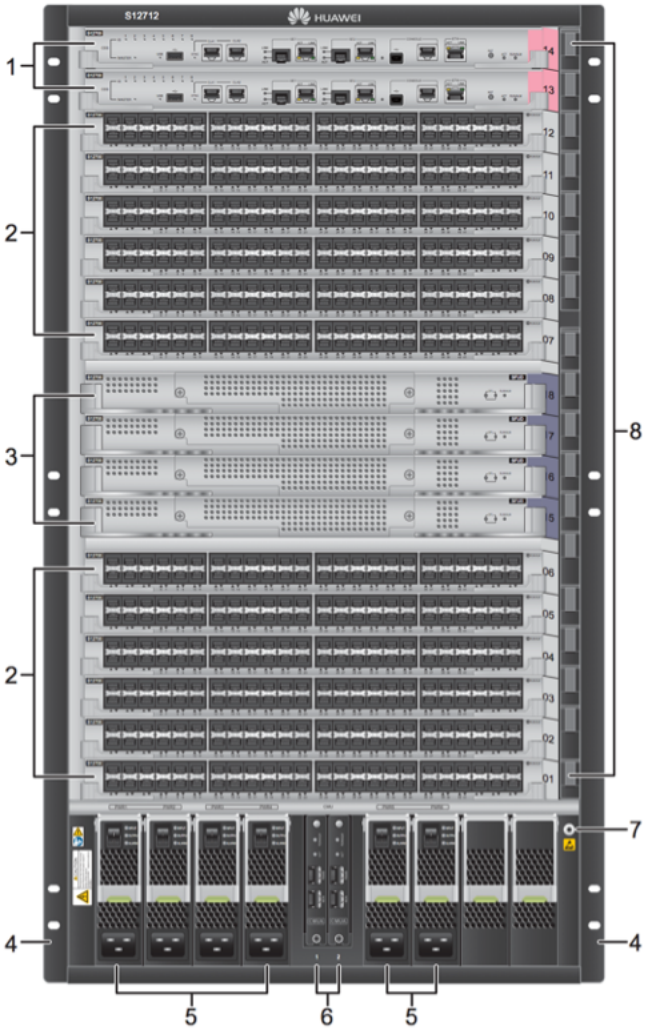
мутаторов доступа. Магистральные каналы, к которым не предъявляется требований по контролю доступа или реализации политик обслуживания, могут формироваться высокопроизводительными картами серии-S или -E, поддерживающими MPLS.

Линейные модули, доступные в текущей модификации S12700 V200R005C00, делятся на группы:

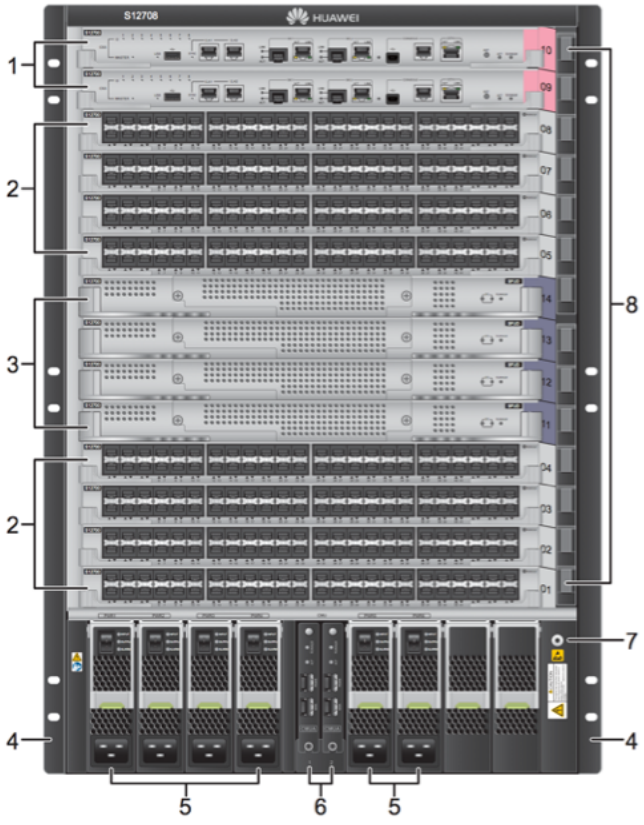
- Firewall модуль – выполняет функции безопасности: Firewall, NAT, IPSec VPN для потока трафика 10, 20 или 40G;
- Open Service Platform Unit (OSPU) – модуль выполняющий интеллектуальные функции по обработке трафика, в том числе CheckPoint IPS и F5 ADC балансировку нагрузки, операционные системы Windows, SUSE и VMware;
- Модуль кластеризации (SFP+ switching system service unit) 8x10G;
- 1000M – интерфейсные модули на 24, 36 или 48 портов GE, могут быть выполнены в серии-S, -E или -X1E (только 48xGE);
- GE/10GE – интерфейсные модули серии-X1E в двух модификациях:
  - 4x10GBASE-X + 24x100/1000BASE-X + 8x10/100/1000BASE-T Combo,
  - 8x10GBASE-X + 8x100/1000BASE-X + 8x10/100/1000BASE-T Combo;
- 10GE – интерфейсные модули на 4, 12 или 16 портов 10GE, могут быть выполнены в серии-S или -E;
- 40GE – интерфейсные модули на 2 или 8 портов 40GE, могут быть выполнены в серии-S.

Шасси и физические характеристики

Шасси коммутатора S12700 существуют в двух модификациях, обеспечивающих соответственно 12 или 8 слотов для линейных карт LPU. В остальном модификации идентичны и поддерживают:



- Два MPU, резервирование 1+1 в шасси или 1+N в кластере коммутаторов, объединенных по технологии CSS2;
- Четыре SFU, резервирование 3+1 в шасси, независимые SFU в каждом коммутаторе кластера;
- До шести модулей электропитания 2200 Вт постоянного или переменного тока в конфигурации резервирования M+N, где число M определяется фактическим энергопотреблением шасси, а N – число резервных модулей;
- Два CMU (Centralized Monitoring Unit) – модулей мониторинга и диагностики, обеспечивающих управление резервированием.



Обозначения на рисунке:

1 – MPU	2 – LPU	3 – SFU	4 – кронштейны для крепежа в стойке
5 – модуль электро-питания	6 – CMU	7 – разъем для браслета заземления	8 – направляющие для кабелей

На рисунке справа показаны направления воздушного потока в шасси коммутатора по типу left-to-back – забор холодного воздуха слева и отдача теплого воздуха через заднюю стенку.

Физические характеристики S12708:

- размеры с рамками для кабелей 442 мм x 585 мм x 664 мм (15 U);
- размеры без рамок 442 мм x 489 мм x 664 мм (15 U);
- максимальное энергопотребление 4,4 кВт;
- вес пустого шасси 19.8 кг;
- максимальный вес 100 кг;
- максимальный шум при нормальной температуре эксплуатации 72 dBA.

Физические характеристики S12712:

- размеры с рамками для кабелей 442 мм x 585 мм x 842 мм (19 U);
- размеры без рамок 442 мм x 489 мм x 842 мм (19 U);
- максимальное энергопотребление 6,6 кВт;
- вес пустого шасси 38.45 кг;
- максимальный вес 130 кг;
- максимальный шум при нормальной температуре эксплуатации 77,9 dBA.

В таблице приведены характеристики модулей S12700:

Тип платы	Наименование	Описание	Максимальное энергопотребление	Вес
MPU	ET1D2MPUA0 00	S12708/ S12712, Main Control Unit A, optional clock	100 W	2.88 kg
SFU	ET1D2SFUA00 0	S12708/ S12712, Switch Fabric Unit A	83 W	3.32 kg
	ET1D2SFUC00 0	S12708, Switch Fabric Unit C	350 W	3.96 kg
	ET1D2SFUD00 0	S12708/ S12712, Switch Fabric Unit D	350 W	3.96 kg
CMU	EH1D200CMU 00	Centralized Monitoring Unit	1W	0.22 kg
OSP	EH1D2PS00P0 0	Open Service Platform Unit	137.5 W	5.50 kg
LPU	ET1D2G24SEC 0	24-port 100/1000BASE -X interface card (EC, SFP)-128K MAC	63 W	2.66 kg
	ET1D2G48TE A0	48-port 10/100/1000BA SE-T interface card (EA, RJ45)-32K MAC	62 W	2.50 kg
	ET1D2G48TE C0	48-port 10/100/1000BA SE-T interface card (EC, RJ45)-128K MAC	68 W	2.62 kg
	ET1D2G48SE A0	48-port 100/1000BASE -X interface card (EA, SFP)-32K MAC	75 W	2.54 kg
	ET1D2G48SEC 0	48-port 100/1000BASE -X interface card (EC, SFP)-128K MAC	92 W	2.66 kg

Тип платы	Наименование	Описание	Максимальное энергопотребление	Вес
	ET1D2T36SEA 0	12-port 100/1000BASE -X and 36-port 10/100/1000BA SE-T interface card (EA, RJ45/ SFP)-32K MAC	62 W	2.50 kg
	ET1D2X04XE A0	4-port 10GBASE-X interface card (EA, XFP)-32K MAC	52 W	2.14 kg
	ET1D2X04XE C1	4-port 10GBASE-X interface card (EC, XFP)-128K MAC	61 W	2.26 kg
	ET1D2X12SSA 0	12-port 10GBASE-X interface card (SA, SFP +)-32K MAC	85 W	2.30 kg
	ET1D2X16SSC 0	16-port 10GBASE-X interface card (SC, SFP +)-128K MAC	150 W	2.60 kg
	ET1D2L02QSC 0	2-port 40GBASE-X interface card (SC, QSFP +)-128K MAC	88 W	2.50 kg
	ET1D2L08QSC 0	8-port 40GBASE-X interface card (SC, QSFP +)-128K MAC	157.2 W	2.80 kg
	ET1D2G48TX1 E	48-port 10/100/1000BA SE-T interface card (X1E, RJ45)	120 W	2.92 kg
	ET1D2G48SX1 E	48-port 100/1000BASE -X interface card (X1E SFP)	140 W	3.04 kg
	ET1D2S04SX1 E	4-port 10GBASE-X and 24-port 100/1000BASE -X and 8-port 10/100/1000BA SE-T combo interface card (X1E, RJ45/ SFP/SFP+)	130 W	2.88 kg
	ET1D2S08SX1 E	8-port 10GBASE-X and 8-port 100/1000BASE -X and 8-port 10/100/1000BA SE-T combo interface card (X1E, RJ45/ SFP/SFP+)	130 W	2.84 kg

Источники питания PAC-2200WF переменного и PDC-2200WF постоянного тока мощностью 2200 Вт. Диапазон электропитания :

- постоянного тока от –38.4В до –72В;
- переменного тока от 90В до 290В.

Спецификации функциональности

Функция		**Описание**
Функции Ethernet	**Ethernet**	Operating modes of full-duplex, half-duplex, and auto- negotiation
		Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, 40 Gbit/ s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)

Функция		Описание
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of access, trunk, hybrid, QinQ, and LNP
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: • MAC address + IP address • MAC address + IP address + interface number • DHCP policies
		VLAN stacking for untagged packets
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VLAN Central Management Protocol (VCMP)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		Configuring MAC address learning priorities for interfaces
		Port bridge
	ARP	Static and dynamic ARP entries
		RARP
		ARP in a VLAN
		Aging of ARP entries
		Proxy ARP
		Multi-port ARP for connecting to the NLB cluster server

Функция		Описание
Ethernet loop protection	**MSTP**	STP
		RSTP
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST
	Loopback- detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
		Single closed ring
		Subring
IPv4/IPv6 forwarding	**IPv4 and unicast routes**	Static IPv4 routes
		VRF
		DHCP client
		DHCP server
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2
		OSPF
		BGP
		MBGP
		IS-IS
		PBR (redirection in a traffic policy)
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM

Функция		Описание
		PIM-SM
		PIM-SSM
		MSDP
		Multicast routing policies
		RPF
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+ & ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
		PIM-SSM for IPv6
	Transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE
Layer 2 multicast features		IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping
		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast
MPLS&VPN	**Basic MPLS functions**	LDP
		Double MPLS labels
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel

Функция		Описание
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes
Device reliability	**BFD**	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	CSS2
	Others	VRRP
Ethernet OAM	**EFM OAM (802.3ah)**	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
	OAM association	Association between 802.1ag and 802.1ah
		Association between 802.1ah and 802.1ag
	Y.1731	Delay and variation measurement
QoS features	**Traffic classifier**	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification

Функция		Описание
		Class-based packet queuing
		Associating traffic classifiers with traffic behaviors
	Traffic policing	Rate limit on inbound and outbound interfaces
	Traffic shaping	Traffic shapping on interfaces and queues
	Congestion avoidance	Weighted Random Early Detection (WRED)
		Tail drop
	Congestion management	Queue mapping
		Priority Queuing (PQ)
		Deficit Round Robin (DRR)
		PQ+DRR
		Weighted Round Robin (WRR)
		PQ+WRR
Configuration and maintenance	**Login and configuration management**	Command line configuration
		Error message and help information in English and Chinese
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		Easy-Deploy (client)
		Easy-Deploy (commander)
		Easy deployment and maintenance
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)

Функция		Описание
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
		Clock features (S12700 supports only Ethernet clock synchronization)
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		Remote in-service upgrade
		In-service patching
Security	**AAA**	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1x authentication
		MAC address authentication
		Portal authentication
		MAC address bypass authentication
	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	IP security	TC-BPDU attack defense
		IP source guard
	CPU	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
		Option 82 function and dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits

Функция		Описание
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management		Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		NetStream
		NAT (SPU)
		Load Balance (SPU)
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2

Показатели производительности

Атрибут	Сервисная функция	Спецификация
Ethernet	Number of MAC addresses supported by each LPU	• EC/SC board: 128K • EA/SA board: 32K • X1E board: 1M
	Number of VLANs	4K
	Number of trunk groups and number of interfaces supported by each trunk group	128 trunk groups, each of which supports a maximum of 8 interfaces • EA/EC/ED board: 128 trunk groups, each of which supports a maximum of 8 interfaces • X1E board: 512 trunk groups, each of which supports a maximum of 32 interfaces
	Number of ARP entries	16K
	Number of ARP entries supported by each LPU	• EA/EC board: 16K • SA board: 8K • SC board: 16K (8K on ET1D2X16SSC0) • X1E board: 256K
QoS	Number of QoS queues on a port	8
	CAR	• EC/EA/SC board: 8 Kbit/s • SA board: 64 Kbit/s • X1E board: 1 Kbit/s

Атрибут	Сервисная функция	Спецификация
ACL	ACLv4	Number of IPv4 ACLs supported by each LPU: • EA board: 6K for inbound traffic; 1K for outbound traffic • EC board: 38K for inbound traffic; 1K for outbound traffic • SA board: 1.5K for inbound traffic; 512 for outbound traffic • SC board: 1K for inbound traffic; 512 for outbound traffic • X1E board: 64K for inbound and outbound traffic • OSP:6K for inbound traffic; 1K for outbound traffic
	ACLv6	Number of IPv6 ACLs supported by each LPU: • EA board: 3K for inbound traffic; 256 for outbound traffic • EC board: 35K for inbound traffic; 256 for outbound traffic • SA board: 512 for inbound traffic; 128 for outbound traffic • SC board: 512 for inbound traffic; 128 for outbound traffic • X1E board: 16K for inbound and outbound traffic • OSP: 3K for inbound traffic; 256 for outbound traffic
MPLS	Number of LSPs	• ED/EC board: 8K • SC board: 4K • Others: not supported
	Number of LDP neighbors	• EA/EC/SC board: 512 local neighbors, 1024 remote neighbors • Others: not supported
L2VPN	Number of VLL entries	2K local connections, 4K remote dynamic connections
	Number of VSI entries	1K
L3VPN	Number of VPN routes	500K
IP unicast	Number of routing entries	3000 k
	IPv4 FIB	• SA board: 12K • EA board: 16K • SC board: 16K • EC board: 128K • X1E board: 3M
	IPv6 FIB	• SA board: 6K • EA board: 8K • SC board: 8K • EC board: 64K • X1E board: 512K
Multicast	Number of static multicast routes	256
	Number of L2 multicast forwarding entries	4K
	Number of L3 multicast forwarding entries	• ED/EC/SC board: 4K • SA board: 2K • X1E board: 128K
Reliability	BFD	• BFD sessions: 2000 • Minimum fault discovery interval: less than 50 ms
	Ethernet OAM	• 802.1ag Up to 64 MDs can be created on the entire system. The number of MAs on the entire system is as follows: 4K Detection time: 3.3 ms • 802.3ah Detection time: 100 ms/1s • Y.1731: microsecond-level latency measurement
	RRPP	• Maximum number of RRPP instances: 64 • Rings supported by the entire system: 64 • Rings supported by each LPU: 12 major rings, 18 subrings • Maximum number of RRPP domains: 64
	VRRP	• VRRP backup groups on the entire system: 255 • Virtual IP addresses in each VRRP backup group: 16 • Switchover time: less than 50 ms when BFD for VRRP is enabled

Атрибут	Сервисная функция	Спецификация
	SmartLink	• Maximum number of instances on the entire system: 64 • Maximum number of Smart Link groups on the entire system: 16 • Switchover time: within 50 ms on optical ports and 3s on electrical ports
	MSTP	• Maximum number of instances on the entire system: 64 • Switchover time: second level
	SEP	• Maximum number of segments on the entire system: 256 • Convergence time: less than 50 ms

Поддержка стандартов

IEEE

Стандарт		Описание
802.1	802.1d	Spanning Tree Protocol
	802.1p	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
	802.1q	Virtual Bridged Local Area Networks
	802.1s	Multiple Spanning Tree Protocol
	802.1w	Rapid Spanning Tree Protocol
	802.1x	Port based network access control protocol
802.3	802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications
	802.3ad	Aggregation of Multiple Link Segments
	802.3ab	Physical Layer Parameters and Specifications for 1000 Mb/s Operation Over 4 Pair of Category 5 Balanced Copper Cabling, Type 1000BASE- T
	802.3ae	10GE WAN/LAN
	802.3af	DTE Power via MIDI
	802.3u	100Base-T
	802.3x	Full Duplex and flow control
	802.3z	Gigabit Ethernet Standard, 1000BASE-X

RFC

Функция	Стандарт	Описание
General Routing Protocols	RFC 768	User Datagram Protocol (UDP)
	RFC 791	Internet Protocol (IP)
	RFC 792	Internet Control Message Protocol (ICMP)
	RFC 793	Transmission Control Protocol (TCP)
	RFC 826	Address Resolution Protocol (ARP)
	RFC 854	Telnet Protocol Specification

Функция	Стандарт	Описание
	RFC 894	Standard for the transmission of IP datagrams over Ethernet networks. C. Hornig. Apr-01–1984. (Format: TXT=5697 bytes) (Also STD0041) (Status: STANDARD)
	RFC 951	Bootstrap Protocol
	RFC 1542	Clarifications and Extensions for the Bootstrap Protocol
	RFC 1027	Using ARP to Implement Transparent Subnet Gateways
	RFC 1122	Requirements for Internet Hosts – Communication Layers
	RFC 1256	ICMP Router Discovery Messages
	RFC 1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
	RFC 1812	Requirements for IP Version 4 Routers
	RFC 2131	Dynamic Host Configuration Protocol
	RFC 2338	Virtual Router Redundancy Protocol (VRRP)
BGP	RFC 1269	Definitions of Managed Objects for the Border Gateway Protocol: Version 3
	RFC 1771	A Border Gateway Protocol 4 (BGP-4)
	RFC 1965	Autonomous System Confederations for BGP
	RFC 1966	BGP Route-Reflection
	RFC 1997	BGP Community Attribute
	RFC 2385	TCP MD5
	RFC 2439	BGP Route Flap Damping
	RFC 2796	BGP Route Reflection
	RFC 2842	Capabilities Advertisement with BGP-4
IP Multicast	RFC 1112	Host extensions for IP multicasting
	RFC 1122	Requirements for Internet Hosts – Communication Layers
	RFC 2236	Internet Group Management Protocol, Version 2
	RFC 2283	Multiprotocol Extensions for BGP-4
	RFC 2362	Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
	draft-ietf- pim-dm-new-v2–02	Protocol Independent Multicast – Dense Mode (PIM-DM)
IS-IS	RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
	RFC 2763	Dynamic Hostname Exchange Mechanism for IS-IS
	RFC 2966	Domain-wide Prefix Distribution with Two-Level IS-IS
MPLS	RFC 2211	Specification of the Controlled-Load Network Element Service
	RFC 2702	Requirements for Traffic Engineering Over MPLS
	RFC 2547	BGP/MPLS VPNs
	RFC 2961	RSVP Refresh Overhead Reduction Extensions

Функция	Стандарт	Описание
	RFC 3031	Multiprotocol Label Switching Architecture
	RFC 3032	MPLS Label Stack Encoding
	RFC 3036	LDP Specification
OSPF	RFC 1583	OSPF Version 2 (obsoletes RFC 1247/obsoleted by RFC 2178)
	RFC 1587	The OSPF NSSA Option
	RFC 1765	OSPF Database Overflow
	RFC 1850	OSPF Version 2 Management Information Base
	RFC 1997	BGP Community Attribute
	RFC 2178	OSPF Version 2 (obsoletes RFC 1583/obsoleted by RFC 2328)
	RFC 2328	OSPF Version 2 (obsoletes RFC 2178)
	RFC 2370	The OSPF Opaque LSA Option
	RFC 2385	TCP MD5
	RFC 2439	BGP Route Flap Damping
	RFC 2842	Capabilities Advertisement with BGP-4
	RFC 2918	Route Refresh Capability for BGP-4
RIP	RFC 1058	Routing Information Protocol
	RFC 2453	RIP Version 2
Denial-of-Service (DoS) Protection	RFC 2267	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (Obsolete)
Network Management	RFC 854	Telnet Protocol Specification
	RFC 951	Bootstrap Protocol
	RFC 1155	Structure and identification of management information for TCP/ IP-based internets
	RFC 1157	A Simple Network Management Protocol (SNMP)
	RFC 1212	Concise MIB Definitions
	RFC 1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
	RFC 1215	A Convention for Defining Traps for use with the SNMP
	RFC 1256	ICMP Router Discovery Messages
	RFC 1493	Definitions of Managed Objects for Bridges
	RFC 1573	Evolution of the Interfaces Group of MIB-II
	RFC 1643	Definitions of Managed Objects for the Ethernet-like Interface Types
	RFC 1650	Definitions of Managed Objects for the Ethernet-like Interface Types using SMIv2
	RFC 1657	Basic BGP4 MIB
	RFC 1724	RIP Version 2 MIB Extension

Функция	Стандарт	Описание
	RFC 1757	Remote Network Monitoring Management Information Base
	RFC 1850	OSPF Version 2 Management Information Base
	RFC 1901	Introduction to Community-based SNMPv2
	RFC 1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
	RFC 2021	Remote Network Monitoring Management Information Base Version 2 using SMIv2
	RFC 2233	The Interfaces Group MIB using SMIv2
	RFC 2668	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
	RFC 2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
	RFC 2925	Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations
Security	RFC 1492	An Access Control Protocol, Sometimes Called TACACS
	draft- grant-tacacs-02	TACACS+
	RFC 2138	Remote Authentication Dial In User Service (RADIUS)